APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,470	10/30/2001	Wei-Qiang Michael Gui	13768.209	9272

47973   7590   12/10/2008
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER
DEBNATH, SUMAN

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>30 September 2008</u>.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-14 and 22-45</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-14 and 22-45</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-14 and 22-45 are pending in this application.

2.   Claims 1-14 and 22-44 are presently amended.

Claim Rejections - 35 USC § 103

3.   Claims 1, 4-5, 9-11, 27, 30-31, 35-37, 41-45 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Moreh et al. (Patent No.: US 6,959,336 B2) (hereinafter

"Moreh") and further in view of Sweet at al. (Pub. No.: US 2002/0031230 A1)

(hereinafter "Sweet") and Seamons et al. (Pub. No.: US 2002/0016777 A1) (hereinafter

"Seamons").

4.   As to claim 1, Moreh discloses in a system including a service that is accessed

by a user from one or more devices with varying input capabilities, a method for

associating multiple credentials with a single user account such that the user may be

authenticated with any one of the multiple credentials (abstract), the method comprising

an authentication system performing acts of:

receiving an authentication request at the authentication system from a device,

wherein the authentication request includes credentials of the user (FIG. 1, col. 5, lines

45-50 and col. 6, lines 5-10);

validating the credentials provided by the user, wherein the credentials are

associated with a single unique user identifier of the user (col. 6, lines 10-20),

receiving new credentials from the user, wherein the new credentials are

associated with the same unique_user identifier of the user (col. 6, lines 32-40),

storing the new credentials in a credential store of the authentication system

such that the authentication system can authenticate the user to the service when the

user provides any one of the multiple credentials (col. 6, lines 32-50); and

Moreh doesn't explicitly disclose that the credentials being selected by the user

from among a plurality of credentials valid at the authentication system and associated

with the user, the credential being chosen by the user based at least partially on the

user's device; the credentials are associated with a single unique user identifier, a user

account, and a user profile, providing, in response to the request the unique user

identifier and the user profile to the device. However, Sweet discloses that the

credentials are associated with a single unique user identifier, a user account, and a

user profile ([0025], [0026], [0039], lines 4-7, [0040], lines 20-26), providing, in response

to the request the unique user identifier and the user profile to the device ([0026],

[0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh as taught by Sweet in

order to "provide a system design which is substantially more compatible with a broad

number of Internet-based applications in the corporate information protection, content

vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,

[0020])"

Neither, Moreh nor Sweet explicitly discloses the credentials being selected by the user from among a plurality of credentials valid at the authentication system and associated with the user, the credential being chosen by the user based at least partially on the user's device. However, Seamons discloses the credentials being selected by the user from among a plurality of credentials valid at the authentication system and associated with the user, the credential being chosen by the user based at least partially on the user's device ([0032], which describes enabling clients to select a set of credentials whose submission will authorize the desired service). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Sweet as taught by Seamons in order to support multiple credential services to client in order to increase the security wherein "the client can issue a second request for service with those credentials attached, and upon verifying the credentials, the server provides the desired service (Seamons, [0032])."

5.   As to claim 4, Moreh doesn't explicitly disclose wherein the act of receiving new credentials from the user further comprises an act of symmetrically associating the new credentials with a unique user identifier. However, Sweet discloses wherein the act of receiving new credentials from the user further comprises an act of symmetrically associating the new credentials with a unique user identifier ([0025], [0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the
time of the invention was made to modify the teaching of Moreh as taught by Sweet in
order to "provide a system design which is substantially more compatible with a broad
number of Internet-based applications in the corporate information protection, content
vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,
[0020])"

6.   As to claim 5, Moreh doesn't explicitly disclose wherein the act of symmetrically
associating the new credential with a unique_user identifier further comprises an act of
associating the new credentials with a user account. However, Sweet discloses wherein
the act of symmetrically associating the new credential with a unique_user identifier
further comprises an act of associating the new credentials with a user account ([0025],
[0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the
time of the invention was made to modify the teaching of Moreh as taught by Sweet in
order to "provide a system design which is substantially more compatible with a broad
number of Internet-based applications in the corporate information protection, content
vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,
[0020])"

7.   As to claim 9, Moreh discloses in a system that includes multiple services that
are accessed by a user over a network such as the Internet, wherein the user accesses

the multiple services from one or more devices that have varying input capabilities, a

method for accessing a service from a device (abstract), the method comprising acts of:

providing multiple credentials to an authentication system, wherein each of the

multiple credentials that is maintained by the authentication system (FIG. 1, col. 6, lines

10-56);

requesting access to a service using a device included in the one or more devices,

wherein the service requires that the user be authenticated before access to the service

is granted to the user, wherein the device is redirected to the authentication system (col.

5, lines 38-56 and col. 6, lines 7-20);

selecting an access credential to send to the authentication system from the multiple

credentials and entering the access credential in the device (col. 6, lines 62-67 to col. 7,

lines 1-4);

issuing an authentication request to an authentication system, wherein the

authentication request includes the access credential selected by the user (col. 7, lines

15-28, col. 9, lines 49-52);

receiving an authentication response from the authentication system, wherein the

authentication response includes the unique user identifier that authenticates the user to

the service if the access credential is validated (col. 6, lines 13-20); and

sending an authenticated request to the service, wherein the authenticated

request includes the unique user identifier such that access to the service is obtained

(col. 6, lines 13-25).

Moreh doesn't explicitly disclose that the credentials being selected by the user from among the multiple credentials provided by the user to the authentication system, the selection based at least partially on the user's device to send to the authentication system and entering the access credential selected by the user in the device; each of the multiple credentials is associated with a user account, a unique user identifier and a user profile. Authentication response also including profile and sending authenticated request with user profile. However, Sweet discloses that each of the multiple credentials is associated with a user account, a unique user identifier and a user profile ([0025], [0026], [0040]). Authentication response also including profile and sending authenticated request with user profile ([0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh as taught by Sweet in order to "provide a system design which is substantially more compatible with a broad number of Internet-based applications in the corporate information protection, content vending, entertainment, and telecommunications (wireless systems) fields (Sweet, [0020])."

Neither, Moreh nor Sweet explicitly discloses the credentials being selected by the user from among the multiple credentials provided by the user to the authentication system, the selection based at least partially on the user's device to send to the authentication system and entering the access credential selected by the user in the device. However, Seamons discloses the credentials being selected by the user from among the multiple credentials provided by the user to the authentication system, the

selection based at least partially on the user's device to send to the authentication

system and entering the access credential selected by the user in the device ([0032],

which describes enabling clients to select a set of credentials whose submission will

authorize the desired service). Therefore, it would have been obvious to one of ordinary

skill in the art at the time of the invention was made to modify the teaching of Moreh and

Sweet as taught by Seamons in order to support multiple credential services to client in

order to increase the security wherein "the client can issue a second request for service

with those credentials attached, and upon verifying the credentials, the server provides

the desired service (Seamons, [0032])."

8.   As to claim 10, Moreh discloses wherein the act of selecting an access credential

to send to an authentication system from multiple credentials further comprises an act of

selecting the access credential according to an input capability of the device (col. 6,

lines 62-67 to col. 7, lines 1-4).

9.   As to claim 11, Moreh discloses wherein the access credential is a numerical

credential when the device has numerical input (col. 6, lines 62-67 to col. 7, lines 1-4).

10.   As to claim 27, it is rejected using the same rationale as for the rejection of claim

1.

11.   As to claim 30, it is rejected using the same rationale as for the rejection of claim

4.

12.   As to claim 31, it is rejected using the same rationale as for the rejection of claim

5.

13.   As to claim 35, it is rejected using the same rationale as for the rejection of claim

9.

14.   As to claim 36, it is rejected using the same rationale as for the rejection of claim

10.

15.   As to claim 37, it is rejected using the same rationale as for the rejection of claim

11.

16.   As to claim 41, Moreh doesn't explicitly disclose wherein the same unique user

identifier is provided to the user regardless of the credentials received from the user.

However, Sweet discloses wherein the same unique user identifier is provided to the

user regardless of the credentials received from the user ([0026], [0039], lines 4-7,

[0040], lines 20-26).

        Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh as taught by Sweet in

order to "provide a system design which is substantially more compatible with a broad

number of Internet-based applications in the corporate information protection, content

vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,

[0020])"

17.   As to claim 42, Moreh doesn't explicitly disclose wherein different credentials are

required from each of the one or more devices. However, Sweet discloses wherein

different credentials are required from each of the one or more devices ([0028]).

        Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh as taught by Sweet in

order to "provide a system design which is substantially more compatible with a broad

number of Internet-based applications in the corporate information protection, content

vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,

[0020])"

18.   As to claim 43, Moreh doesn't explicitly disclose wherein providing the unique

user identifier and the user profile to the device comprises sending a cookie containing

the unique user identifier and the user profile to the device. However, Sweet discloses

wherein providing the unique user identifier and the user profile to the device comprises

sending a cookie containing the unique user identifier and the user profile to the device

([0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the
time of the invention was made to modify the teaching of Moreh as taught by Sweet in
order to "provide a system design which is substantially more compatible with a broad
number of Internet-based applications in the corporate information protection, content
vending, entertainment, and telecommunications (wireless systems) fields. (Sweet,
[0020])"

19.   As to claim 44, Moreh doesn't explicitly disclose wherein the user profile includes
data about the user comprising name, personal information, preferred language,
preferences, and location. However, Sweet discloses wherein the user profile includes
data about the user comprising name, personal information, preferred language,
preferences, and location.

20.   As to claim 45, Neither, Moreh nor Sweet explicitly discloses wherein the act of
validating the credentials provided by the user further comprises an act of the
authentication system comparing the credentials selected by the user against the
credentials stored in the credential store to determine validity. However, Seamons
discloses wherein the act of validating the credentials provided by the user further
comprises an act of the authentication system comparing the credentials selected by
the user against the credentials stored in the credential store to determine validity
([0032], which describes enabling clients to select a set of credentials whose
submission will authorize the desired service). Therefore, it would have been obvious to

one of ordinary skill in the art at the time of the invention was made to modify the

teaching of Moreh and Sweet as taught by Seamons in order to support multiple

credential services to client in order to increase the security wherein "the client can

issue a second request for service with those credentials attached, and upon verifying

the credentials, the server provides the desired service (Seamons, [0032])."

21.   Claims 2-3, 8, 12, 22, 25-26, 28-29, 34 and 38 are rejected under 35

U.S.C. 103(a) as being unpatentable over Moreh and further in view of Sweet, Seamons

and Wood et al. (Patent No.: US 6,609,198 B1) (hereinafter "Wood").

22.   As to claims 2, Moreh discloses wherein the act of receiving an authentication

request at the authentication system further comprises an act of determining where to

send the credentials for validation (col. 6, lines 10-20). Neither Moreh nor Sweet and

Seamons explicitly disclose that the authentication system is a distributed authentication

system. However, Wood discloses that the authentication system is a distributed

authentication system (col. 17, lines 15-25).

        Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh, Sweet and Seamons

as taught by Wood in order to provide enhanced security to the credential repository

with location transparency.

23.   As to claim 3, Moreh discloses wherein the act of determining where to send the

credentials for validation uses a username of the credentials (col. 6, lines 5-55).

24.   As to claim 8, Moreh discloses further comprising one or more of:

        a step for remembering which credential was received in the authentication

request (col. 6, lines 5-40);

        Neither Moreh nor Sweet and Seamons explicitly discloses a step for prompting

the user for a more secure credential when the credentials received in the

authentication request do not meet security requirements of the service; and a step for

providing at least one security measure for each credential associated with the user

account, wherein the user is not authenticated to a service if the security measure of a

particular credential is breached or the user account is locked. However, Wood

discloses a step for prompting the user for a more secure credential when the

credentials received in the authentication request do not meet security requirements of

the service (col. 10, lines 25-65); and a step for providing at least one security measure

for each credential associated with the user account, wherein the user is not

authenticated to a service if the security measure of a particular credential is breached

or the user account is locked (col. 10, lines 30-35).

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Moreh, Sweet and Seamons as

taught by Wood in order to provide credentials without loss of session continuity.

25.   As to claim 12, neither Moreh nor Sweet and Seamons explicitly disclose the
method further comprising:

an act of requiring the user to provide a secure credential to the authentication
system that is more secure than the access credential; and

an act of providing the service with a level of security of the secure credential and
of the access credential, wherein the service is unaware of both the selected credential
and the secure credential.

However, Wood discloses an act of requiring the user to provide a secure
credential to the authentication system that is more secure than the access credential
(col. 10, lines 25-65); and

an act of providing the service with a level of security of the secure credential and
of the access credential, wherein the service is unaware of both the selected credential
and the secure credential (col. 10, lines 25-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the
time of the invention was made to modify the teaching of Moreh, Sweet and Seamons
as taught by Wood in order to provide credentials without loss of session continuity.

26.   As to claim 22, Moreh doesn't explicitly discloses wherein the new credential has
an associated security level and wherein the method further comprises:

associating the new credential with the user account such that the user can be
authenticated with both the original credential and the new credential,

prior to providing the response, and subsequent to receiving the authorization

request, prompting the user for a secure credential that is more secure than the original

credential if the security level of the original credential is insufficient for a service being

accessed by the user, wherein the service is provided with the security level of both the

original credential and the secure credential, but is not aware of either the original

credential or the secure credential.

However, Sweet discloses wherein the new credential has an associated security

level and wherein the method further comprises:

associating the new credential with the user account such that the user can be

authenticated with both the original credential and the new credential ([0025], [0026],

[0040]). Authentication response also including profile and sending authenticated

request with user profile ([0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh as taught by Sweet in

order to "provide a system design which is substantially more compatible with a broad

number of Internet-based applications in the corporate information protection, content

vending, entertainment, and telecommunications (wireless systems) fields (Sweet,

[0020])."

Neither Moreh nor Sweet and Seamons explicitly discloses prior to providing the

response, and subsequent to receiving the authorization request, prompting the user for

a secure credential that is more secure than the original credential if the security level of

the original credential is insufficient for a service being accessed by the user, wherein

the service is provided with the security level of both the original credential and the

secure credential, but is not aware of either the original credential or the secure

credential.

However, Wood discloses prior to providing the response, and subsequent to

receiving the authorization request, prompting the user for a secure credential that is

more secure than the original credential if the security level of the original credential is

insufficient for a service being accessed by the user, wherein the service is provided

with the security level of both the original credential and the secure credential, but is not

aware of either the original credential or the secure credential (col. 10, lines 25-65).

Therefore, it would have been obvious to one of the ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh, Sweet and Seamons

as taught by Wood in order to provide credentials without loss of session continuity.

27.   As to claim 25, Moreh discloses further comprising a step for automatically

authenticating the user at different services after the user has been authenticated at a

first service (col. 15, lines 10-30, "….federated authentication source that ultimately

leads to global single sing-on").

28.   As to claim 26, Moreh discloses wherein the original credential is a numerical

credential when the device has a preferred numerical input (col. 6, lines 62-67 to col. 7,

lines 1-4).

29.   As to claim 28, it is rejected using the same rationale as for the rejection of claim

2.

30.   As to claim 29, it is rejected using the same rationale as for the rejection of claim

3.

31.   As to claim 34, it is rejected using the same rationale as for the rejection of claim

8.

32.   As to claim 38, it is rejected using the same rationale as for the rejection of claim

12.

33.   Claims 7, 14, 33 and 40 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Moreh and further in view of Sweet, Seamons and Leah et al. (Patent

No.: US 6,986,039 B1) (hereinafter "Leah").

34.   As to claim 7, neither Moreh nor Sweet and Seamons explicitly disclose wherein

the act of receiving new credentials from the user further comprises an act of

asymmetrically associating the new credentials with a primary credential, wherein the

primary credential is stored in a primary store with the unique user identifier. However,

Leah discloses wherein the act of receiving new credentials from the user further

comprises an act of asymmetrically associating the new credentials with a primary

credential, wherein the primary credential is stored in a primary store with the unique

user identifier (FIG. 3, col. 10, lines 48-67 to col. 11, lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh, Sweet and Seamons

as taught by Leah in order to synchronize credentials securely and propagate among

multiple directories, operating system platforms and registries.

35.   As to claim 14, neither Moreh nor Sweet and Seamons explicitly disclose wherein

the authentication system is a distributed system and wherein some of the multiple

credentials are stored on different credential stores, wherein the act of providing

multiple credentials to an authentication service further comprises an act of

asymmetrically associating the multiple credentials with a primary credential, wherein

the unique user identifier is stored with the primary credential.

However, Leah discloses wherein the authentication system is a distributed

system and wherein some of the multiple credentials are stored on different credential

stores, wherein the act of providing multiple credentials to an authentication service

further comprises an act of asymmetrically associating the multiple credentials with a

primary credential, wherein the unique user identifier is stored with the primary

credential (FIG. 3, col. 10, lines 48-67 to col. 11, lines 1-10, which describes validating

credentials with master credentials).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Moreh, Sweet and Seamons

as taught by Leah in order to synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.

36.   As to claim 33, it is rejected using the same rationale as for the rejection of claim 7.

37.   As to claim 40, it is rejected using the same rationale as for the rejection of claim 14.

38.   Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in view of Sweet, Seamons, Wood and Leah.

39.   As to claim 23, neither Moreh nor Sweet, Seamons and Wood explicitly discloses wherein the step for associating new credential with the user account further comprises a step for symmetrically associating the original credential and the new credential with the user account, wherein the user account is cached with each of the original credential and the new credential.

However, Leah discloses wherein the step for associating new credential with the user account further comprises a step for symmetrically associating the original credential and the new credential with the user account, wherein the user account is cached with each of the original credential and the new credential (col. 10, lines 48-67 to col. 11, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Sweet, Seamons and Wood as taught by Leah in order to synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.

40.   As to claim 24, neither Moreh nor Sweet, Seamons and Wood explicitly discloses wherein the step for associating the new_credential with the user account further comprises a step for asymmetrically associating the new credential with a primary credential, wherein the primary credential is associated with the user account and wherein the primary credential is cached with each new credential.

However, Leah discloses wherein the step for associating the new_credential with the user account further comprises a step for asymmetrically associating the new credential with a primary credential, wherein the primary credential is associated with the user account and wherein the primary credential is cached with each new credential (col. 10, lines 48-67 to col. 11, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Sweet, Seamons and Wood as taught by Leah in order to synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.

41.   Claims 13 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in view of Sweet, Seamons, Laursen and Wood.

42.   As to claim 13, neither Moreh and Sweet nor Seamons explicitly disclose wherein the authentication system is a distributed system and wherein some of the multiple credentials are stored on different credential stores, wherein the act of providing multiple credentials to an authentication service further comprises one or more of: a step for symmetrically associating the multiple credentials with the unique user identifier, wherein the use identifier is cached with each of the multiple credentials; a step for symmetrically associating the multiple credentials with a user account, wherein a user account is cached with each of the multiple credentials and a step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked.

However, Laursen disclose a method wherein some of the multiple credentials are stored on different stores, wherein the act of providing multiple credentials to an authentication service (abstract) further comprises one or more of:

a step for symmetrically associating the multiple credentials with the unique user identifier, wherein the user identifier is cached with each of the multiple credentials (col. 8, lines 4-35);

a step for symmetrically associating the multiple credentials with a user account, wherein a user account is cached with each of the multiple credentials (col. 8, lines 4-35) .

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Sweet as taught by Laursen in order to perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired.

Neither Moreh and Sweet nor Seamons and Laursen explicitly disclose a method wherein the authentication system is a distributed system and a step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked. However, Wood discloses a method wherein the authentication system is a distributed system (col. 17, lines 15-25) and a step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked (col. 10, lines 30-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Sweet, Seamons and Laursen as taught by Wood in order to provide enhanced security to the credential repository with location transparency.

43.   As to claim 39, it is rejected using the same rationale as for the rejection of claim 13.

44.   Claims 6 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Moreh and further in view of Sweet, Seamons and Laursen et al. (Patent No.:

6,065,120) (hereinafter "Laursen").

45.   As to claim 6, neither Moreh nor Sweet explicitly disclose wherein the act of

symmetrically associating the new credential with a unique user identifier further

comprises an act of caching a copy of the unique user identifier with the new credential.

However, Laursen discloses wherein the act of symmetrically associating the new

credential with a unique user identifier further comprises an act of caching a copy of the

unique user identifier with the new credential (FIG. 2b, col. 8, lines 4-35).

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Moreh and Sweet by including an

act of caching a copy of the user identifier with the new credential as taught by Laursen

in order to perform transactions or retrieve pertinent information without the need to key

in such every time the transactions or the information are desired.

46.   As to claim 32, it is rejected using the same rationale as for the rejection of claim

6.

47.   Examiner's note: Examiner has cited particular columns and line numbers in the

references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are

applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

48.   Applicant has amended claims 1-14 and 22-44, please see rejection above.

Conclusion

49.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435